IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

COMCAST CABLE COMMUNICATIONS, LLC, Plaintiff, v. NAGRA USA, INC., NAGRAVISION S.A., KUDELSKI S.A., Defendants.	Case No. 2:17-cv-664 JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Comcast Cable Communications, LLC ("Plaintiff" or "Comcast"), by and through its undersigned attorneys, hereby allege as follows, upon actual knowledge with respect to itself and its own acts, and upon information and belief as to all other matters.

PRELIMINARY STATEMENT

This complaint is part of an on-going dispute between the parties that is centered in this district. On December 5, 2016, Nagravision S.A. brought a complaint for patent infringement against Comcast and its affiliates in this district. Civil Action No. 2:16-cv-1362-JRG. Comcast moved to transfer, but subsequently withdrew that motion after Nagravision S.A. submitted an opposition and declaration detailing the substantial nature of its contacts and presence in this district. Thereafter, Comcast answered the complaint on July 21, 2017.

On August 16, 2017, Comcast sought leave to amend its answer to assert patent infringement counterclaims against Nagravision S.A. and its close affiliates, Kudelski S.A., and Nagra USA, Inc. (hereinafter, collectively "Nagra" or "Defendants"). Specifically, Comcast's counterclaims alleged that Defendants infringed U.S. Patent Nos. 7,620,179 and 7,933,410. The

factual and legal allegations asserted in those proposed counterclaims are substantially identical to the factual and legal allegations asserted herein.

Nagravision S.A. opposed Comcast's motion for leave to amend, arguing that Comcast would not be prejudiced by a denial of its motion because it could file its complaint as a separate action. Aug. 31, 2017 Opp'n to Mot. for Leave to Amend at 8 (Dt. No. 108). On September 20, 2017, United States District Judge for the Eastern District of Texas, Rodney Gilstrap, denied Comcast's motion for leave to add counterclaims, noting that Comcast would not be "unduly prejudice[d]" by denial because it could file its claims in a separate lawsuit. Sept. 20, 2017 Order at 3 (Dkt. No. 123).

By filing this lawsuit, Comcast follows the course of action that Defendants and the Court both proposed. In light of the significant volume of litigation and discovery that has already been conducted in this district relating to this dispute, including the overlap of factual issues relating to the parties' encryption technologies, the efficiencies uniquely call for litigation in this District.

NATURE OF THE CASE

1. This is an action for patent infringement under 35 U.S.C. § 271 *et seq.* by Comcast against Defendants Nagra USA, Inc., Nagravision S.A., and Kudelski S.A. (collectively "Defendants" or "Nagra") for their infringement of U.S. Patent Nos. 7,620,179 ("'179 Patent") and 7,933,410 ("'410 Patent") (collectively, "the Comcast Patents").

2. Nagra directly infringes the Comcast Patents by, among other things, making, using, offering for sale, or selling within the United States, and/or importing into the United States, conditional-access systems and services.

3. Nagra indirectly infringes the Comcast Patents through the direct-infringement

activities of its customers or the subscribers of those customers.

4. Comcast seeks damages, injunctive, and other relief for Nagra's willful infringement.

PARTIES

5. Comcast is a limited liability company organized and existing under the laws of the State of Delaware with its principal place of business in Philadelphia, Pennsylvania. Comcast provides video, high-speed Internet, and voice services to residential subscribers under the XFINITY brand.

6. On information and belief, Defendant Nagravision S.A. is a Swiss corporation with its principal place of business and headquarters in Cheseaux-sur-Lausanne, Switzerland. On information and belief, Nagravision S.A. is the digital television division of the "Kudelski Group."

7. On information and belief, Defendant Nagra USA, Inc. is a New York corporation with its principal place of business and headquarters in El Segundo, California.

8. On information and belief, Defendant Kudelski S.A. is a Swiss corporation with its principal place of business of business and headquarters in Cheseaux-sur-Lausanne, Switzerland. On information and belief, Defendant Nagra USA, Inc. and Defendant Nagravision S.A. are wholly-owned subsidiaries of Kudelski S.A.

9. On information and belief, Defendants have acted in combination, and/or as one another's agents and/or alter egos, to commit acts of infringement in this district and elsewhere. Defendants publicly hold themselves out as members of "the Kudelski Group," and publicly hold out "Kudelski's NAGRA subsidiaries" as the Kudelski Group's providers of technology relating to conditional access systems (CAS), which perform security-related functions, primarily for cable and satellite television providers. On information and belief, members of the Kudelski

Group frequently blur the lines of their corporate separateness. For example, officers and employees of one Kudelski entity are authorized to, and frequently do, perform official actions on behalf of other Kudelski entities, including without limitation Defendants Kudelski S.A., Nagravision S.A., and Nagra USA, Inc. Moreover, on information and belief, each Defendant entity's business operations are performed by their co-defendant, based on geographic convenience. On information and belief, this blurring of corporate separateness also occurs in this district.

JURISDICTION AND VENUE

10. The Court has subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a) with respect to claims arising under the patent laws, 35 U.S.C. §§ 1 *et seq*.

11. This Court has personal jurisdiction over Defendants. On information and belief, Defendants conduct business and have committed and continue to commit acts of infringement in this district and elsewhere in the United States by making, using, offering for sale, selling, and/or importing Nagra conditional-access systems and services.

12. Venue is proper as to Nagravision S.A. and Kudelski S.A. at least because each is a foreign corporation subject to personal jurisdiction in this district. Venue is proper as to Nagra USA, Inc., at least because, on information and belief, it has a regular and established place of business in this district and has acted in combination with, and/or as the agent or alter ego of, Nagravision S.A. and Kudelski S.A. to commit acts of infringement in this district.

BACKGROUND

13. Comcast provides video, high-speed Internet, and voice services to residential and business customers under the XFINITY brand. It is one of the largest video, high-speed Internet, and phone providers to residential customers in the world.

14. Comcast has been a leader in the field of data security in connection with its video

and TV services. It has devoted a substantial amount of research and development to the security of data transmitted using those services. Comcast also developed the Comcast Innovation Fund, which provides substantial funding for researchers at leading academic institutions and elsewhere to support research in the data security and related fields.

15. As a result of its research and development efforts, Comcast has contributed numerous inventions to the industry. Many of its inventions relate to securing television and video signals that are delivered to consumer homes using secure channels and innovative security-related technologies. The patents at issue in this Complaint are among the important advances that arose from Comcast's dedicated research and development in this area.

16. Nagra has provided and continues to provide conditional-access systems and services to various customers such as satellite and cable television providers in the United States, including on information and belief DISH Network, Altice USA, and CableOne. Nagra's conditional-access systems and services include Nagra CONNECT, Persistent Rights Management (PRM or DRM), Nagravision Advanced Security Certification (NASC), Nagravision On-Chip Security (NOCS), Nagra COMMAND, anyCAST, anyCAST COMMAND, and anyCAST CONNECT. On information and belief, Nagra uses, tests, has used and has tested such systems and services in the United States. Furthermore, on information and belief, Nagra or its customers incorporate such Nagra systems and services into set-top boxes and receivers distributed for use by the customers and their subscribers.

17. Upon information and belief, Nagra requires its customers or their subscribers to allow or facilitate Nagra ongoing-oversight responsibility so that Nagra can exert continuing direction or control over Nagra conditional-access systems and services after deployment. *See, e.g.*, Nagra's description of its certification and specification requirements at pages 10–14 of

"Nagra Media PRM – A Solution for the Delivery and Persistent Storage of Protected Content" (available at http://docplayer.net/14949739-Nagra-media-prm-a-solution-for-the-delivery-and-persistent-storage-of-protected-content.html) (herein "Nagra PRM Presentation"). Nagra exerts such continuing direction or control over its customers or the customers' subscribers.

18. Nagra has infringed and continues to infringe the Comcast Patents by, among other things, making, using, testing, offering for sale, selling, leasing, or offering to lease in the United States, or importing into the United States, infringing conditional-access systems and services to its customers or to its customers' subscribers.

19. Nagra has had knowledge of each of the Comcast Patents and its infringement, as well as the infringement by its customers or their subscribers, since at least August 15, 2017 when it was informed by Comcast of the Comcast Patents and the infringing nature of the Nagra conditional-access systems and services. Thus, Nagra knows and has known (or was willfully blind to the fact) that its customers or their subscribers have been infringing and continue to infringe each of the Comcast Patents in conjunction with the Nagra conditional-access systems or services implemented in their intended manner as instructed by Nagra.

20. Nagra's past and continuing infringement was and is willful.

FIRST CLAIM FOR RELIEF
(Infringement of U.S. Patent No. 7,620,179)

21. Paragraphs 1-20 are incorporated herein by reference.

22. The '179 Patent is titled "System and Method for Security Processing Media Streams." The '179 Patent issued on November 17, 2009 to James Fahrny and Charles Compton. A true and correct copy of the '179 Patent is attached as Exhibit A.

23. The original assignee of the '179 Patent was Comcast Cable Holdings, LLC. Plaintiff is the current owner by assignment of all right, title, and interest of the '179 Patent.

24. The ’179 Patent is directed to multi-stream security-processing involving decryption and encryption using a controller in a receiver such as a set-top box that is programmed through downloads from a headend.

25. Claim 9 of the ’179 Patent recites:

> A method of multi-stream security processing and distributing digital media streams, the method comprising:
>
> generating encrypted digital media streams at a headend;
>
> coupling a network to the headend and receiving the encrypted digital media streams at the network;
>
> coupling a receiver to the network, the receiver receiving a software download from the network;
>
> receiving the encrypted digital media streams at the receiver, and presenting a decrypted version of the encrypted digital media streams using the receiver;
>
> re-configuring a security processor in the receiver based on the software download to provide at least one of simultaneous multiple encryption and simultaneous multiple decryption processing of the digital media streams; and
>
> storing the software download in the security processor;
>
> wherein the security processor comprises a plurality of digital stream encryption/decryption engines that are selectively coupled by a controller for simultaneous operation in response to a predetermined security configuration;
>
> wherein the security configuration comprises at least one of Data Encryption Standard (DES), Triple DES (3-DES), Advanced Encryption Standard (AES), and Common Scrambling Algorithm (CSA).

26. Upon information and belief, Nagra infringes at least method claim 9 of the ’179 Patent through the making, manufacture, use, testing, offer for sale, sale, lease, or offer to lease in the United States, or importation into the United States, of infringing conditional-access systems and services.

27. Specifically, upon information and belief, Nagra has and is providing in the United States conditional-access and security-processing services to customers including DISH Network LLC, Altice USA, Inc., or Cable ONE, Inc. *See* https://www.nagra.com /media-center/press-releases/nagravision-and-dish-network-sign-new-long-term-agreement;

https://dtv.nagra.com/altice-usa-selects-nagra-content-protection-us-cable-operations; https://www.nagra.com/sites/default/files/RA_2016_E.pdf.

28. Upon information and belief, through its conditional-access systems and services, Nagra has used and uses its customers' networks to send scrambled or encrypted digital media streams from a headend to Nagra's code in the customer's receiver, such as a set-top box:

> PRM protects Video on Demand (VoD) content, including adaptively streamed content whether VoD or "Live". VoD encompasses both Push-VoD (content is pushed to the device storage unit before the end-user may purchase it), Pull-VoD (content is loaded to the device storage unit upon end-user request only) and streamed content (content is rendered immediately and not stored permanently).
>
> The system encrypts content at the head-end and generates entitlements uniquely associated with the target device[5]. PRM works with a wide range of mechanisms to transport the content from the head-end to the device, and does not place specific limitations on such delivery.

See Nagra PRM Presentation at Section 2.2 (p. 6).

29. Upon information and belief, Nagra code is incorporated in, for example, a Broadcom 7445 chip in certain set-top boxes. *See* http://www.digitaltvnews.net/?p=25852; http://www.technewsworld.com/story/83251.html.

30. The Nagra code encrypts and decrypts the received streams (*see, e.g.*, Nagra PRM Presentation) and provides for simultaneous operation across multiple display devices:

> NAGRA CONNECT is a single, converged CAS/DRM client that fully supports the multi-network, multi-device, multi-use case reality, thereby reducing complexity and cost. It can be implemented on set-top boxes, open devices or selected Connected TVs, and also includes the ability to secure Netflix streaming to STBs. It's approved by third-party auditors and Hollywood studios for 4K Ultra HD, and is used by some of the world's most advanced cable, satellite and telco service providers.

See https://dtv.nagra.com/secure/casdrm; *see also* http://www.digitaltvnews.net/?p=25852.

31. Upon information and belief, Nagra periodically downloads authenticated updates from a headend to the Nagra code in its customers' (or their subscribers') receivers and set-top boxes in order to re-configure or modify the Nagra code:

of entitlements already delivered, hence disabling a device from accessing content. All devices are required to support secure software updates to enable renewability.

See Nagra PRM Presentation at Section 6.1.2 (p. 15).

The device manufacturer:

- Shall provide the right to perform software updates free of charge to the device and must provide support for such updates, if needed, under a time and expenses agreement.

See Nagra PRM Presentation at Section 5 (p. 14).

32. Upon information and belief, Nagra stores its authenticated updates in flash memory:

4.3.1 Software Boot and Download Protection

An important certification step centers around the software booting and software download authentication processes. These must correctly leverage signature checking features in the NOCS chipset. NASC includes:

- Preventing modifications on the boot loader code and validating the code during boot by using the signature process.
- Preventing download of non-authorized code in flash memory and validating the update software using the signature process.

See Nagra PRM Presentation at Section 4.3.1 (p. 12).

33. Upon information and belief Nagra's code uses at least the Advanced Encryption Standard (AES):

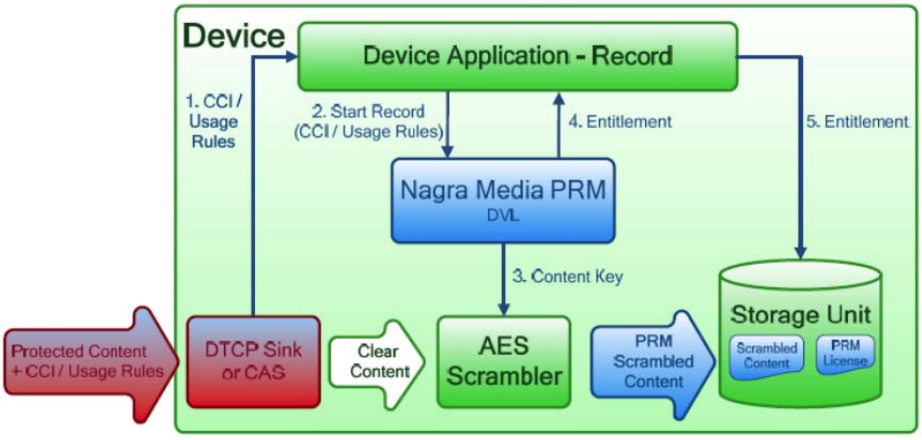

Figure 3 – DVR Recording

See Nagra PRM Presentation (p. 9).

34. Upon information and belief, Nagra directs or controls its customers or their

subscribers, or requires its customers or their subscribers to allow or facilitate ongoing Nagra oversight responsibility and control for implementing, maintaining, updating or using the security processing performed by the Nagra code. *See, e.g.*, Nagra PRM Presentation at pages 10–14. On information and belief, additional examples of ongoing Nagra control include periodically renewing, updating, or facilitating updating of, Nagra code via the headend connection, sending credentials and entitlements to its code that provide for the encrypted exchange of video content between devices, and monitoring for any third-party attempt to circumvent Nagra security measures. *Id*. & documents cited therein, including "Nagra Advanced Security Certification," "PRM Specification," and the "standard legal contract."

35. Through its actions, as described above, Nagra has directly infringed and continues to directly infringe at least method claim 9 of the '179 Patent, either literally or under the doctrine of equivalents, under 35 U.S.C. § 271(a).

36. In addition, Nagra is indirectly responsible for the past and continuing direct infringement by certain third parties of at least method claim 9 of the '179 Patent. Such third parties include (a) Nagra customers such as DISH Network LLC, Altice USA, Inc., and Cable ONE, Inc.; and (b) such customer's subscribers. Specifically, when the Nagra conditional-access systems or services are made, used, sold, offered for sale, or imported into the United States, by Nagra customers, or are made or used by subscribers of a Nagra customer, such action constitutes direct infringement of at least method claim 9 of the '179 Patent as described.

37. Furthermore, Nagra has had knowledge of both the '179 Patent and the direct infringement by its customers and their subscribers since at least August 15, 2017, when it was informed by Comcast of the patent and the infringing nature of the Nagra conditional-access systems and services. Thus, Nagra knows and has known (or was willfully blind to the fact) that

its customers (or their subscribers) directly infringe claims of the ’179 Patent through their making, using, offering to sell, or selling within the United States, or importing into the United States, the Nagra conditional-access systems or services. Additionally, Nagra has had knowledge of the ’179 Patent and has known or been willfully blind to the foregoing third-party direct infringement since at least the filing of this Complaint and the contentions herein.

38. Nagra has specifically intended to induce, and has induced, its customers and their subscribers to directly infringe at least claim 9 of the ’179 Patent, and has known or been willfully blind to that infringement, through Nagra’s advice and assistance to its customers and their subscribers in the use of the Nagra conditional-access systems or services.

39. Upon information and belief, Nagra provides instructional and other explanatory materials to its customers or their subscribers that describe the proper implementation and use of the Nagra conditional-access systems or services, including in, for example, the “PRM Specification” and “NASC Specification” documents referenced at page 14 of the Nagra PRM Presentation. Upon information and belief, Nagra actively encouraged and continues to actively encourage its customers or their subscribers to directly infringe the ’179 Patent by manufacturing, making, using, testing, importing, selling, and/or leasing the Nagra conditional-access systems or services, as well as: marketing the Nagra conditional-access systems or services to its customers or their subscribers, including on its website www.nagra.com; promoting the security features in those systems; working with its customers or their subscribers to implement and install the Nagra conditional-access systems or services; and supporting, managing, and providing technical assistance to them during their use.

40. Thus, Nagra has induced, and continues to induce, infringement under 35 U.S.C. § 271(b) of at least claim 9 of the ’179 Patent.

41. Further, Nagra has contributorily infringed, and continues to contributorily infringe, under 35 U.S.C. § 271(c), at least claim 9 of the ’179 Patent. As explained, certain third parties, including Nagra customers and those customers’ subscribers, have been and are now infringing, including under 35 U.S.C. § 271(a), at least claim 9 of the ’179 Patent.

42. Nagra makes, uses, sells, offers to sell, or leases to its customers the Nagra conditional-access systems or services, which are especially made or adapted by Nagra to be used as a component, material or apparatus of the claims of the ’179 Patent and have no non-infringing use. For example, as explained, Nagra provides code for the Nagra conditional-access systems or services to its customers or their subscribers, which are integrated into set-top boxes or receivers used as part of television services in a manner that infringes the ’179 Patent.

43. Upon information and belief, the functionality in the Nagra code is not a staple article or commodity of commerce. Because the code is designed to work only in a manner that is covered at least by claim 9 the ’179 Patent, it has no substantial noninfringing use. At least since August 15, 2017, Nagra also has known or been willfully blind to the fact that such functionality is especially made and adapted for, and is used in, a manner covered by the ’179 Patent.

44. As a result of Nagra’s acts of direct, indirect, and willful infringement of the ’179 Patent, Comcast has suffered and will continue to suffer monetary damages, including lost profits or a reasonable royalty, that are compensable under 35 U.S.C. § 284 in an amount to be determined at trial.

45. Unless an injunction is issued enjoining Nagra and its officers, directors, agents, servants, affiliates, employees, divisions, branches subsidiaries, parents, and all others acting on its behalf from infringing the ’179 Patent, Comcast will continue to be irreparably harmed.

Moreover, the balance of hardships between Comcast and Nagra, and the public interest, warrants such an injunction.

SECOND CLAIM FOR RELIEF
(Infringement of U.S. Patent No. 7,933,410)

46. Paragraphs 1-45 are incorporated herein by reference.

47. The ’410 Patent is titled “System and method for a variable key ladder.” The ’410 Patent issued on April 26, 2011 to James Fahrny. A true and correct copy of the ’410 Patent is attached as Exhibit B.

48. The original assignee of the ’410 Patent was Comcast Cable Holdings, LLC. Plaintiff is the current owner by assignment of all right, title, and interest of the ’410 Patent.

49. The ’410 Patent is directed to an apparatus and method for generating encryption and decryption keys in connection with a key ladder. In one embodiment, for example, the apparatus and method relate to storing a device key and one or more other keys, decrypting and/or extracting another device key from a data message using the first device key, and using a key ladder that may comprise, for example, the device key to decrypt a data stream.

50. Claim 4 of the ’410 Patent recites:

> A method for decrypting a data stream, comprising:
>
> storing configuration data and at least some of a plurality of keys, wherein a first one of the keys is a symmetric device key and a second one of the keys is an asymmetric key;
>
> receiving, by a receiver, a data stream including a data message;
>
> generating a third one of the keys as another device key by decrypting the data message using the second one of the keys;
>
> selecting between the first one of the keys and the third one of the keys depending on the configuration data; and
>
> decrypting at least a portion of the data stream using a key ladder that includes the selected first or third one of the keys.

51. Upon information and belief, Nagra infringes at least claim 4 of the ’410 Patent

through the making, manufacture, use, testing, offer for sale, sale, lease, or offer to lease in the United States, or importation into the United States, of infringing conditional-access systems and services.

52. Specifically, upon information and belief, Nagra has and is providing conditional-access and security-processing services to at least DISH Network LLC, Altice USA, Inc., or Cable ONE, Inc. in the United States. *See* https://www. nagra.com/media-center/press-releases/nagravision-and-dish-network-sign-new-long-term-agreement; https://dtv.nagra.com/altice-usa-selects-nagra-content-protection-us-cable-operations; https://www.nagra.com/sites/default/files/ RA_2016_E.pdf.

53. Upon information and belief, through its conditional-access systems or services, Nagra has used and uses its customers' networks to send scrambled or encrypted digital media streams from a headend to Nagra's code in the customer's receiver, such as a set-top box:

> PRM protects Video on Demand (VoD) content, including adaptively streamed content whether VoD or "Live". VoD encompasses both Push-VoD (content is pushed to the device storage unit before the end-user may purchase it), Pull-VoD (content is loaded to the device storage unit upon end-user request only) and streamed content (content is rendered immediately and not stored permanently).
>
> The system encrypts content at the head-end and generates entitlements uniquely associated with the target device[5]. PRM works with a wide range of mechanisms to transport the content from the head-end to the device, and does not place specific limitations on such delivery.

See Nagra PRM Presentation at Section 2.2 (p. 6).

54. Upon information and belief, Nagra code is incorporated in, for example, a Broadcom 7445 chip in certain set-top boxes. *See* http://www.digitaltvnews.net/?p=25852; http://www.technewsworld.com/story/83251.html.

55. The Nagra code encrypts and decrypts the received streams (*see, e.g.*, Nagra PRM Presentation) and provides for simultaneous operation across multiple display devices:

> NAGRA CONNECT is a single, converged CAS/DRM client that fully supports the multi-network, multi-device, multi-use case reality, thereby reducing complexity and cost. It can be implemented on set-top boxes, open devices or selected Connected TVs, and also includes the ability to secure Netflix streaming to STBs. It's approved by third-party auditors and Hollywood studios for 4K Ultra HD, and is used by some of the world's most advanced cable, satellite and telco service providers.

See https://dtv.nagra.com/secure/casdrm; *see also* http://www.digitaltvnews.net/?p=25852.

56. Upon information and belief, Nagra periodically downloads authenticated updates from a headend to the Nagra code in its customers' (or their subscribers') receivers and set-top boxes in order to re-configure or modify the Nagra code:

> of entitlements already delivered, hence disabling a device from accessing content. All devices are required to support secure software updates to enable renewability.

See Nagra PRM Presentation at Section 6.1.2 (p. 15).

> The device manufacturer:
>
> - Shall provide the right to perform software updates free of charge to the device and must provide support for such updates, if needed, under a time and expenses agreement.

See Nagra PRM Presentation at Section 5 (p. 14).

57. Upon information and belief, the Nagra conditional-access systems or services allow, for example, video-on-demand (VOD) content encrypted at a head end to be delivered securely to such receivers and set-top boxes for subsequent decryption and viewing:

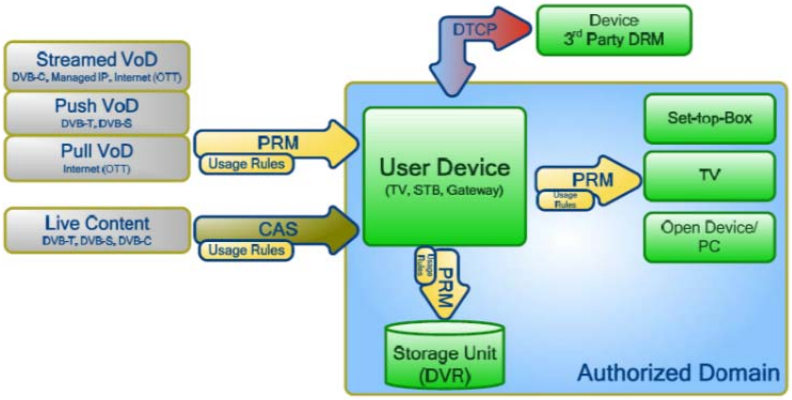

Figure 1 – Nagra Media PRM: Persistent Right Management

See Nagra PRM Presentation (p. 5).

58. Upon information and belief, Nagra stores keys and configuration data in memory such as Flash memory, ROM, RAM, and/or registers. For example, it stores data that is general to the network, services, content, device, and protocols; conditional-access configuration data; and/or other data that is unique to a consumer set-top box/receiver or its operation. The Nagra conditional-access systems or services also utilize data for configuring keys, encryption methods, and key ladders used during the various encryption and decryption processes. *See, e.g.*, Nagra PRM Presentation at Section 2.2 (pp. 5, 11).

59. Upon information and belief, the Nagra conditional-access systems or services employ the various stored keys for decrypting content. In order to access protected content, for example, the Nagra conditional-access systems or services utilize a symmetric device key. *See, e.g.*, *id.* (p. 5). They also utilize asymmetric keys as part of the encryption and decryption process. *See, e.g.*, *id.* Also, when used or tested, the set-top box/receiver receives a data stream, such as for example video-on-demand content and entitlement data, that comprises one or more data messages.

60. The Nagra conditional-access systems or services further include decryption operator for generating a third key as another device key. For example, as explained in the

"Nagra Media PRM – A Solution for the Delivery and Persistent Storage of Protected Content" specification, the head end scrambles video-on-demand or other data stream content using a key that relates to the subscriber's set-top box/receiver. The key is obtained by decrypting a data message using the asymmetric key referenced above. *See, e.g.*, *id.* (pp. 5, 6).

61. Upon information and belief, the Nagra conditional-access systems or services employ a switch that selects keys depending on the configuration data. If, among other things, the key is being used to decrypt the entitlement message, the Nagra conditional-access systems or services select the first key for decryption. If, among other things, the key is being used to decrypt the scrambled content, they select the third key. See, for example:

> Access to protected content requires a valid credential, PRM cryptography is based on the presence of a unique secret in the device hardware. This secret allows PRM to create a specific entitlement that can only be decrypted by a specific device. In addition, in VOD use cases, entitlements are signed to ensure both the integrity and that they were created in the Nagra head-end.
>
> **Content Protection**
>
> Any piece of content recorded or received on the device is encrypted. Recorded content protection is done as soon as CAS, DTCP or other link protection is removed. PRM uses one scrambling key per asset.

Nagra PRM Presentation (p. 5).

62. Upon information and belief, the Nagra conditional-access systems or services functionality includes computer code and/or hardware (i.e., a decryption engine) for decrypting a portion of the data stream. *See, e.g.*, Nagra PRM Presentation (p. 6) ("This entitlement is generated by the PRM head-end components upon request for a specific content item by a specific device. . . . A portal handling the viewer's VoD purchase typically performs the delivery of this entitlement to the device, which can be through a range of delivery mechanisms."). The data stream is decrypted using, for example, the third device key. *See, e.g.*, *id.* (p. 9).

63. Upon information and belief, and as explained above, at least the third device key is part of a key ladder used to decrypt the data stream. *See, e.g.*, *id.* (p. 12) ("NASC certification

checks that . . . key ladders . . . can be accessed correctly by the software."). An exemplary decryption engine is shown in Fig. 4 of the "Nagra Media PRM – A Solution for the Delivery and Persistent Storage of Protected Content" specification:

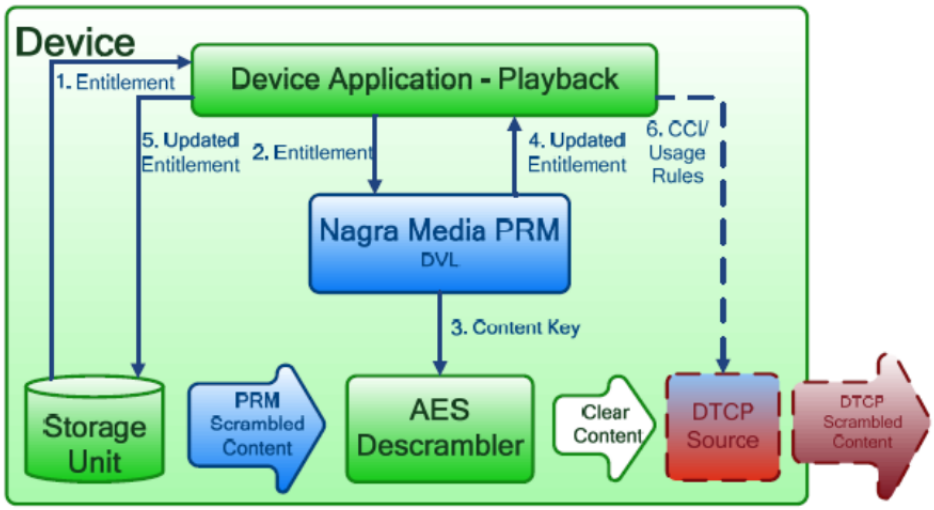

Figure 4 – DVR Playback

Nagra PRM Presentation) (p. 9).

64. Upon information and belief, Nagra directs or controls its customers or their subscribers, or requires its customers or their subscribers to allow or facilitate ongoing Nagra oversight responsibility and control for implementing, maintaining, updating or using the security processing performed by the Nagra code. *See, e.g.*, Nagra PRM Presentation. On information and belief, additional examples of ongoing Nagra control include periodically renewing, updating, or facilitating updating of, Nagra code via the headend connection, sending credentials and entitlements to its code that provide for the encrypted exchange of video content between devices, and monitoring for any third-party attempt to circumvent Nagra security measures. *Id*. & documents cited therein, including "Nagra Advanced Security Certification," "PRM Specification," and the "standard legal contract.

65. Through its actions, including those described above, Nagra has therefore directly infringed and continues to directly infringe at least claim 4 of the ’410 Patent, either literally or under the doctrine of equivalents, under 35 U.S.C. § 271(a).

66. In addition, Nagra is indirectly responsible for the past and continuing direct infringement by certain third parties of claims of the ’410 Patent. Such third parties include (a) Nagra customers such as DISH Network LLC, Altice USA, Inc., and Cable ONE, Inc.; and (b) such customers’ subscribers. Specifically, when the Nagra conditional-access systems or services are made, used, sold, offered for sale, or imported into the United States, by Nagra customers, or are made or used by subscribers of a Nagra customer, such action constitutes direct infringement of at least claim 4 of the ’410 Patent.

67. Furthermore, Nagra has had knowledge of both the ’410 Patent and the direct infringement by its customers and their subscribers since at least August 15, 2017, when it was informed by Comcast of the patent and the infringing nature of the Nagra conditional-access systems and services. Thus, Nagra knows and has known (or was willfully blind to the fact) that its customers’ (and their subscribers’) directly infringe claims of the ’410 Patent through their making, using, offering to sell, or selling within the United States, or importing into the United States, the Nagra conditional-access systems or services. Additionally, Nagra has had knowledge of the ’410 Patent and has known or been willfully blind to the foregoing third-party direct infringement since at least the filing of this Complaint and the contentions herein.

68. Nagra has specifically intended to induce and has induced its customers and their subscribers to directly infringe at least claim 4 of the ’410 Patent, and has known or been willfully blind to that infringement, through Nagra’s advice and assistance to its customers and their subscribers in the use of the Nagra conditional-access systems or services.

69. Upon information and belief, Nagra provides instructional and other explanatory materials to its customers or their subscribers that describe the proper implementation and use of the Nagra conditional-access systems or services, including in, for example the "PRM Specification" and "NASC Specification" documents referenced at p.14 of the Nagra PRM Presentation. Upon information and belief, Nagra actively encouraged and continues to actively encourage its customers and their subscribers to directly infringe the '410 Patent by making, manufacturing, using, testing, importing, selling, and/or leasing the Nagra conditional-access systems or services, as well as marketing the Nagra conditional-access systems or services to its customers and their subscribers, including on its website www.nagra.com; promoting the security features in those systems; working with its customers or their subscribers to implement and install the Nagra conditional-access systems or services; and supporting, managing, and providing technical assistance to them during their use.

70. Thus, Nagra has induced, and continues to induce, infringement under 35 U.S.C. § 271(b) of at least claim 4 of the '410 Patent.

71. Further, Nagra has contributorily infringed, and continues to contributorily infringe, under 35 U.S.C. § 271(c) at least claim 4 of the '410 Patent. As explained, certain third parties, including Nagra customers and those customers' subscribers, have been and are now infringing, including under 35 U.S.C. § 271(a), at least claim 4 of the '410 Patent.

72. Nagra sells or leases to its customers the Nagra conditional-access systems or services, which are especially made or adapted by Nagra to be used as a component, material or apparatus of the claimed invention of the '410 Patent and have no other non-infringing uses. For example, as explained, Nagra provides code for the Nagra conditional-access systems or services to its customers or their subscribers, which are integrated into set-top boxes or receivers used as

part of television services in a manner that infringes the ’410 Patent.

73. Upon information and belief, the functionality in the Nagra code is not a staple article or commodity of commerce. Because the code is designed to work only in a manner that is covered by at least claim 4 the ’410 Patent, it has no substantial noninfringing use. At least since August 15, 2017, Nagra has also known or been willfully blind to the fact that such functionality is especially made and adapted for, and is used in, a manner covered by the ’410 Patent.

74. As a result of Nagra’s acts of direct, indirect, and willful infringement of the ’410 Patent, Comcast has suffered and will continue to suffer monetary damages, including lost profits or a reasonable royalty, that are compensable under 35 U.S.C. § 284 in an amount to be determined at trial.

75. Unless an injunction is issued enjoining Nagra and its officers, directors, agents, servants, affiliates, employees, divisions, branches subsidiaries, parents, and all others acting on its behalf from infringing the ’410 Patent, Comcast will continue to be irreparably harmed. Moreover, the balance of hardships between Comcast and Nagra, and the public interest, warrants such an injunction.

JURY DEMAND

Comcast hereby demands a jury trial on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Comcast respectfully requests the Court to enter judgment in its favor and against Defendants as follows:

A. A judgment that Defendants have infringed at least claim 10 of the ’179 Patent, literally and/or under the doctrine of equivalents;

B. A judgment that Defendants’ infringement of the ’179 Patent has been willful;

C. An order permanently enjoining Defendants and their officers, directors, agents, servants, affiliates, employees, divisions, branches subsidiaries, parents, and all others acting in active concert therewith from infringement of the ’179 Patent;

D. An award to Comcast of all damages caused by Defendants’ infringement of the ’179 Patent;

E. A judgment that Defendants have infringed at least claim 4 of the ’410 Patent, literally and/or under the doctrine of equivalents;

F. A judgment that Defendants’ infringement of the ’410 Patent has been willful;

G. An order permanently enjoining Defendants and their officers, directors, agents, servants, affiliates, employees, divisions, branches subsidiaries, parents, and all others acting in active concert therewith from infringement of the ’410 Patent;

H. An award to Comcast of all damages caused by Defendants’ infringement of the ’410 Patent;

I. An award of all pre-judgment and post-judgment interest on the damages caused by Defendants’ infringement of the Comcast Patents;

J. A declaration that this case is exceptional under 35 U.S.C. § 285;

K. An award of Comcast’s costs and attorneys’ fees incurred in this action; and

L. Further relief as the Court may deem just and proper.

Dated: September 22, 2017

Respectfully submitted,

By: */s/ Robert A. Van Nest*

Robert A. Van Nest
David J. Silbert (*pro hac vice* forthcoming)
Brian L. Ferrall (*pro hac vice* forthcoming)
Leo L. Lam (*pro hac vice* forthcoming)
Ajay Krishnan (*pro hac vice* forthcoming)
Ryan K. Wong (*pro hac vice* forthcoming)
David Rosen (*pro hac vice* forthcoming)
Taylor Gooch (*pro hac vice* forthcoming)
Shayne Henry (*pro hac vice* forthcoming)
KEKER, VAN NEST & PETERS LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400
Facsimile: (415) 397-7188
rvannest@keker.com
dsilbert@keker.com
bferrall@keker.com
llam@keker.com
akrishnan@keker.com
rwong@keker.com
drosen@keker.com
tgooch@keker.com
shenry@keker.com

Deron R. Dacus (Texas Bar No. 790553)
THE DACUS FIRM, P.C.
821 ESE Loop 323, Suite 430
Tyler, Texas 75701
Telephone: (903) 705-1117
Facsimile: (903) 581-2543
ddacus@dacusfirm.com

Attorneys for Plaintiff
COMCAST CABLE COMMUNICATIONS, LLC